WHAT IS CLAIMED IS:

1. An encryption/decryption apparatus comprising:

a plurality of encryption function portions which are provided in parallel to each other, output cipher text data by encrypting plain text data based on key data in accordance with each block, and/or output plain text data by decrypting cipher text data based on key data in accordance with each block; and

a plurality of means for generating key data which generate key data by converting a common key based on an intermediate processing result of any encryption function portions and any one of two or more types of conversion processing different from each other, and input generated key data to any encryption function portion which is yet to start processing.

2. The encryption/decryption apparatus according to claim 1, wherein said each conversion processing converts said common key based on any one of two or more variable data different from each other.

3. An encryption/decryption apparatus comprising:

a plurality of encryption function portions which are provided in parallel to each other, output cipher text data by encrypting plain text data based on key data in accordance with each block, and/or output plain data by decrypting cipher text data based on key data in accordance with each block; and

a plurality of key data generation portions

configured to generate key data by converting a common key based on an intermediate processing result of any encryption function portion and any one of two or more types of conversion processing different from each other, and input generated key data to any encryption function portion which is yet to start processing.

4. The encryption/decryption apparatus according to claim 3, wherein said each conversion processing converts said common key based on any one of two or more variable data different from each other.

5. An authenticating apparatus for generating an authenticator from a message and authenticating said message based on said authenticator, comprising:

a plurality of encryption function portions which are provided in parallel to each other and create cipher text data by encrypting said message based on key data in accordance with each block;

a plurality of means for generating key data which generate key data by convert a common key based on an intermediate processing result of any encryption function portion and any one of two or more types of conversion processing different from each other, and individually input generated key data to any encryption function portion which is yet to start processing; and

an authenticator generation portion which generates said authenticator based on cipher text data generated by an encryption function portion at a last

stage.

6. The authenticating apparatus according to claim 5, wherein said each conversion processing converts said common key based on any one of two or more variable data different from each other.

7. An authenticating apparatus for generating an authenticator from a message and authenticating said message based on said authenticator, comprising:

a plurality of encryption function portions which are provided in parallel to each other, which generate cipher text data by encrypting said message based on key data in accordance with each block;

a plurality of key data generation portions configured to generate key data by converting a common key based on an intermediate processing result of any encryption function portion and any one of two or more types of conversion processing different from each other, and individually input generated key data to any encryption function portion which has yet to start processing; and

an authenticator generation portion which generates said authenticator based on cipher text data generated by an encryption function portion at a last stage.

8. The authenticating apparatus according to claim 7, said each conversion processing converts said common key based on any one of two or more variable

data different from each other.

9. A computer program stored in a computer-readable storage medium used in an encryption/decryption apparatus, comprising:

a first program code which causes a computer to sequentially execute a plurality of types of encryption function processing for outputting cipher text data by encrypting plain text data based on key data in accordance with each block and/or outputting plain text data by decrypting cipher text data based on key data; and

a second program code for causing said computer to sequentially execute a plurality of types of key data generation processing for converting a common key based on an intermediate processing result of any encryption function processing and any one of two or more types of conversion processing different from each other and inputting generated key data to any encryption function processing which has yet to start processing.

10. The computer program according to claim 9, wherein said each conversion processing converts said common key based on any one of two or more variable data different from each other.

11. A computer program which generates an authenticator from a message and is stored in a computer-readable storage medium used in an authenticating apparatus for authenticating said

message based on said authenticator, comprising:

a first program code for causing a computer to sequentially execute a plurality of types of encryption function processing for generating cipher text data by encrypting said message based on key data in accordance with each block;

a second program code for causing said computer to sequentially execute a plurality of types of key data generation processing for converting a common key based on an intermediate processing result of any encryption function processing and any one of two or more conversion processing different from each other and inputting generated key data to any encryption function processing which is yet to start processing; and

a third program code for causing said computer to execute authenticator generation processing for generating said authenticator based on cipher text data generated by encryption function processing on a last stage.

12. The computer program according to claim 11, wherein said each conversion processing converts said common key based on any one of two or more variable data different from each other.

13. An encryption/decryption method comprising:

outputting cipher text data by subjecting plain text data to encryption processing based on key data in accordance with each block in parallel, and outputting

plain text data by subjecting cipher text data to decryption processing based on key data in accordance with each block in parallel; and

generating key data by converting a common key based on an intermediate processing result of encryption processing or decryption processing on a preceding stage and any one of a plurality of types of conversion processing and inputting generated key data to encryption processing or decryption processing on a subsequent stage.

14. The encryption/decryption method according to claim 13, wherein said each conversion processing converts said common key based on any one of a plurality of variable data.

15. An authenticating method for generating an authenticator from a message and authenticating said message based on said authenticator, comprising:

generating cipher text data by subjecting said message to encryption processing based on key data in accordance with each block in parallel;

converting a common key based on an intermediate processing result of encryption processing on a preceding stage and any one of a plurality of types of conversion processing, and individually inputting generated key data to any encryption processing on a subsequent stage; and

generating said authenticator based on cipher text

data generated by encryption processing on a last stage.

16. The authenticating method according to claim 15, wherein said each conversion processing converts said common key based on any one of a plurality of variable data.